

# Internal Audit Report

## CGI - Enterprise Architecture

31 March 2023

CS2207

**Overall  
Assessment**

**Substantial  
Assurance**

# Contents

- Executive Summary ..... 3
- Audit Assessment ..... 4
- Background and scope ..... 5
- Findings and Management Action Plan..... 6
- Appendix 1 – Control Assessment and Assurance Definitions ..... 10

This Internal Audit review is conducted for the City of Edinburgh Council under the auspices of the 2022/23 internal audit plan approved by the Governance, Risk and Best Value Committee in March 2022. The review is designed to help the City of Edinburgh Council assess and refine its internal control environment. It is not designed or intended to be suitable for any other purpose and should not be relied upon for any other purpose. The City of Edinburgh Council accepts no responsibility for any such reliance and disclaims all liability in relation thereto.

The internal audit work and reporting has been performed in line with the requirements of the Public Sector Internal Audit Standards (PSIAS) and as a result is not designed or intended to comply with any other auditing standards.

Although there are specific recommendations included in this report to strengthen internal control, it is management’s responsibility to design, implement and maintain an effective control framework, and for the prevention and detection of irregularities and fraud. This is an essential part of the efficient management of the City of Edinburgh Council. Communication of the issues and weaknesses arising from this audit does not absolve management of this responsibility. High and Critical risk findings will be raised with senior management and elected members as appropriate.

## Overall Opinion and summary of findings

Our review confirmed that whilst some control weaknesses were identified in the design and effectiveness of the Enterprise Architecture function, they provide reasonable assurance that risks are being managed. Requirements are well defined within the Output Based Specification 17 (OBS 17) agreement, Enterprise Architecture and across the CGI Contract Schedules.

There is scope to improve the linkage between the strategic principles defined by the Council and the architecture principles utilised during the design of solutions, and to ensure that the Architecture Principles, that support the framework are reviewed according to the agreed review cycle.









Four low rated findings have been identified as follows:

- ICT Architecture Principles mapping to the IT Strategy: a mapping exercise has been conducted between the ICT Architecture Principles and IT Strategic Principles. It is noted that a mapping should be performed of the high-level principles against the strategy to ensure alignment with the design principles.
- Enterprise Architecture documentation: the Architecture Principles have not been updated since 2019, following their initial creation and approval. A review is scheduled for 2023.
- Chief Technology Officer (CTO) responsibilities: the role of CTO within CGI should be clarified to ensure agreement between Digital Services and CGI on how that role will be fulfilled.
- Compliance with OBS Architecture clauses: while a joint review process exists, not all OBS 17 clauses are currently fully compliant.

## Areas of good practice identified

- CGI provides an Annual Architecture Summary report that details an overview of the Technology Estate and current issues being actioned, as well as a summary of investments made across the Council's key functions (e.g., Housing, City Infrastructure & Place, Waste & Cleansing). The report details the investments made across the key IT principles to:
  - extend and leverage the functionality of recent investments
  - invest and establish new enterprise capabilities
  - consolidate to reduce estate complexity
  - retain and manage the estate.
- Higher Level Design (HLD) documents follow a consistent structure that document the principles leveraged, architectural decisions taken, the function and non-functional requirements and collaboration with other functions (e.g., testing, service operations and security) to deliver the solution.
- The Council provides a comprehensive review of the HLD documents through a review summary template that is reviewed by the CGI Solution Architect and actioned. The Council review forms an ongoing review whereby HLDs are not signed off until the Council Technical Architect approves the document.
- An exception process is in place to capture risks and issues identified through the review summary template and the Joint Design Authority (JDA). Risk assessments are performed to review the issue and propose mitigation actions that are re-reviewed by the JDA, furthermore, approval can be provided to either send the HLD back for re-work, approve the HLD or approve with exceptions which are managed through a risk entry in the CGI RiskIT portal.

# Audit Assessment

Audit Area	Control Design	Control Operation	Findings	Priority Rating
1. Architecture Function			Finding 1: ICT Architecture Principles mapping to the IT Strategy Finding 2: Periodic review of ICT Architecture Principles documents	<b>Low Priority</b>
2. Architecture Governance			Finding 3: Performing additional CTO responsibilities as per OBS 17	<b>Low Priority</b>
3. Architecture Board			No findings identified	<b>N/A</b>
4. Architecture Compliance			Finding 4: Compliance with OBS Architecture clauses	<b>Low Priority</b>

[See Appendix 1 for Control Assessment and Assurance Definitions](#)

# Background and scope

The Enterprise Architecture function within the City of Edinburgh Council (the Council) is managed by CGI (the Council's external technology partner) who provide services to the council according to the agreed Outcome Based Specification (OBS) contractual agreement and other contractual schedules. The OBS agreement details 22 functional requirements that CGI will provide to satisfy CEC's minimum requirements. These span across several areas including:

- providing an initial Operating Level Agreement (OLA) that details the relationship to be provided, roles and responsibilities, skills, and reporting
- a formal governance structure that includes a Joint Authority and Design Board
- production of ICT principles that are aligned to the strategic needs of CEC, that are reviewed yearly and re-defined based on any significant changes to the ICT or business strategies
- production of Higher Level and Lower-Level Design documents which are aligned to the ICT principles to describe the technical solutions proposed
- an exception process to manage solution designs that are progressed outside of the ICT principles.

The OBS document contains a requirement for joint creation of an OLA which details the forums in place to support the Enterprise Architecture function. An Enterprise Architecture Board is in place to review the technical direction of the function, to ensure alignment between business and Digital Services strategies, developing technology trends and the ICT principles.

In addition, a Design Authority is in place to review Higher Level Design documents, provide challenge and approval before delivery into production.

## Scope

This review focused predominantly on the adequacy and effectiveness of the key controls supporting the definition of the enterprise architecture function, governance in place, including the Joint Design Authority, over the enterprise architecture function and architecture compliance activities. The review also considered how the enterprise architecture framework had been embedded into Higher Level Design documentation.

## Risks

- strategic delivery
- technology and information
- service delivery

## Limitations of Scope

The following areas were excluded from scope:

- The review of individual projects and their compliance to the overall Enterprise Architecture framework is out of scope of this review.
- As the audit did not assess all requirements within OBS 17, this should be considered a sample assessment.

## Reporting Date

Testing was undertaken between 1 November 2022 and 10 February 2023. Our audit work concluded on 10 February 2023, and our findings and opinion are based on the conclusion of our work as at that date.

# Findings and Management Action Plan

Finding Rating	Low priority
----------------	--------------

## Finding 1 – ICT Architecture Principles mapping to the IT Strategy

As part of the OBS 17 document, CGI are required to maintain the following ICT Architecture Principles:

- providing a yearly review of ICT principles as a minimum to maintain relevance to the changing needs of the Authority over time (OBS 17.4)
- review of the ICT principles at any time should a significant change in ICT or business strategies occur that requires a change in the approach (OBS 17.4).

CGI maintain three ICT Architecture principles which supplement the OBS 17 document:

- Application Architecture: which describes 19 principles to support solution design, including considering vendor or cloud hosting, utilising plug and play integration and ensuring applications are integrated with standard patterns.
- Data Architecture: which describes four principles that ensure data is managed for its intended use, is treated as a public asset, and is designed to connect with other datasets to drive insights.
- Security Architecture: which describes 14 principles to build resilience into solutions.

These principles are leveraged during the design of new solutions or architectural changes.

Seven IT Strategic Principles have also been developed and agreed as part of the Digital and Smart Cities strategy (2020-23) which provide a framework for future technology services, inform investment decisions, and drive the roadmap for the next year. Review of the ICT Architecture Principles notes a broad alignment with the IT Strategic Principles.

CGI provided a spreadsheet with a mapping exercise that, had been conducted between the ICT Architecture Principles and IT Strategic Principles. It is noted though, that this mapping is high level and does not demonstrate, how it will naturally be applied to the design principles to ensure alignment.

In addition, the mechanism to review the architecture principles has not been performed since 2019 which is in contrary to the timescales set out in the Operating Level Agreement (OLA) (see finding 2). It is noted that the Digital and Smart City Strategy will be reviewed in 2023.

### Risks

- **Strategic Delivery / technology and information** – updates made at a strategic level may not be reflected in the underlying principles that are leveraged for the design of solutions leading to solutions being developed outside of the Council’s strategic intentions.

## Recommendations and Management Action Plan: Principles Mapping

Recommendation 1.1	Agreed Management Action	Action Owners	Contributors	Timeframe
<p>CGI and Digital Services should perform a mapping of the Enterprise Architecture principles aligned to the renewed 2023 Digital and Smart City Strategy.</p> <p>If Architecture Principles remain that do not map back to an IT Strategic Principle, a rationale should be provided that justifies its inclusion to support solution design against the desired business outcomes.</p>	<p>CGI &amp; DS will perform a mapping of Architecture principles against the renewed 2023 Digital and Smart City Strategy.</p> <p>CGI &amp; DS will review the design principles in line with agreed EA plan.</p>	<p>Deborah Smart, Executive Director of Corporate Services, CEC</p> <p>Mark Bulmer, Vice President Consulting Services, CGI</p>	<p>Nicola Harvey, Service Director, Customer and Digital Services</p> <p>Heather Robb, Chief Digital Officer, Digital Services</p> <p>Mike Bell, Technical Architect, Digital Services</p> <p>Alison Roarty, Commercial Lead, Digital Services</p> <p>Iain Allan, Enterprise Architect, CGI</p>	<p>31/03/2024</p>

## Finding 2 – Periodic review of ICT Architecture Principles documents

Finding  
Rating

Low priority

The Operating Level Agreement (OLA), which has been agreed between CGI and the Council, and reviewed in 2022, states that the periodic review of Architecture Principles should occur every six months and IT Strategic Principles should be reviewed every year.

Review of the three principles relating to application, data, and security architecture, provided by CGI, noted that these documents have not undergone a review since 2019, when the principles were created and initially agreed to align with the development of the Councils Digital and Smart City Strategy (2020-23), which is outside the six-month review period documented within the OLA.

CGI / Digital Services have advised that in line with OBS 17.3 the principles should be reviewed every year or in response to significant strategic change with the principles currently under review to align with development of the refreshed Digital and Smart City Strategy in 2023.

### Risks

- **Strategic Delivery / technology and information** – updates required to be made to the ICT Architecture Principles because of significant business changes may not be captured leading to solutions being designed utilising out of date principles that do not accurately reflect the intentions of the Council.

## Recommendations and Management Action Plan: Periodic review of ICT Architecture Principles documents

Recommendation 2.1	Agreed Management Action	Action Owner	Contributors	Timeframe
The Operating Level Agreement (OLA) should be reviewed to ensure it accurately reflects the requirements and timescales for reviewing Architecture and IT strategic principles, as agreed, and understood by CGI and the Council.	CGI & DS will review the OLA in line with overall EA plan.	Deborah Smart, Executive Director of Corporate Services, CEC  Mark Bulmer, Vice President Consulting Services, CGI	Nicola Harvey, Service Director, Customer and Digital Services Heather Robb, Chief Digital Officer, Digital Services Mike Bell, Technical Architect, Digital Services Alison Roarty, Commercial Lead, Digital Services Iain Allan, Enterprise Architect, CGI	31/01/2024

## Finding 3 – Performing additional CTO responsibilities as per OBS 17

Finding  
Rating

Low priority

The OBS 17 document details the agreed services to be provided by CGI to The Council. OBS 17.1 details the roles and responsibilities of a Chief Technical Officer (CTO), to provide 'strategic advice around business requirements' and the Enterprise Architect, who 'manages the design authority and Authority-retained IT architects'. CGI advised that the CTO role is not currently in place and therefore the following additional activities are not being performed:

- 17.5: Approval from Supplier CTO or named deputy and Authority Design Authority nominee that Higher Level Documents (HLDs) may be published and issued.

CGI and Digital Services have advised that approval of HLDs is performed by the Council's Technical Architect and CGI Enterprise Architect as part of the Joint Design Authority. However, with the absence of a CTO role, the expected responsibility outlined within OBS 17.1 has not defined, on who would carry these out on a periodic basis.

### Risks

- **Strategic Delivery / technology and information** – the CGI CTO, or alternative role does not perform a review of Higher-Level Documents from a strategic perspective to ensure designs are developed in line with the Council strategic direction or against the requirements detailed in the OBS document:

## Recommendations and Management Action Plan: CTO responsibilities

Recommendation 3.1	Agreed Management Action	Action Owner	Contributors	Timeframe
<p>The role of CTO within CGI should be clarified to ensure there is agreement between the Council and CGI on how that role and corresponding activities will be fulfilled to enable alignment with the requirements set out in OBS 17.</p> <p>The agreement should include agreement from CGI that the requirements of the role will be undertaken by senior IT member that has relevant experiences and understanding of the Council's to provide assurance that architecture activities are being performed and reviewed quarterly in line with the Council's strategic intentions.</p> <p>If the intention is that the CTO role will not be fulfilled, an alternative arrangement with clear roles and responsibilities should be documented and agreed by both the Council and CGI.</p>	CGI will define the CTO roles and responsibilities and agree these with DS.	<p>Deborah Smart, Executive Director of Corporate Services, CEC</p> <p>Mark Bulmer, Vice President Consulting Services, CGI</p>	<p>Nicola Harvey, Service Director, Customer and Digital Services</p> <p>Heather Robb, Chief Digital Officer, Digital Services</p> <p>Mike Bell, Technical Architect, Digital Services</p> <p>Alison Roarty, Commercial Lead, Digital Services</p> <p>Iain Allan, Enterprise Architect, CGI</p>	31/03/2024



## Finding 4 – Compliance with OBS Architecture clauses

Finding Rating	Low priority
----------------	--------------

Currently the Council review the entire Enterprise Architecture process detailed in OBS 17 against the artefacts and processes provided by CGI, are tracked in a live planning spreadsheet and reviewed jointly on an ongoing and annual basis during Joint Architecture Board meetings. The objective of this review is to ensure that CGI are delivering to their OBS obligations as per their agreement with Digital services.

The review spreadsheet sheet contains each entry clause from OBS 17, with the Council’s main requirements and against their corresponding deliverables, which are reviewed on agreed set frequencies. The clauses are marked with a status of being colour coded red, amber, or green to depict if it meets non, partial, or full compliance respectively.

Review of the tracker noted a total of 69 OBS clauses with only 21 clauses assessed as fully compliant, with the status for the remaining clauses as follows:

- non-compliant - 8
- partially compliant - 40





### Risks

- **Strategic Delivery / technology and information** – the Council do not have adequate assurance that all OBS architecture clauses are fully met and compliant.

## Recommendations and Management Action Plan: Enterprise Architecture Artefacts – review and remediation

Recommendation 4.1	Agreed Management Action	Action Owner	Contributors	Timeframe
<p>The Council should ensure the planned reviews of Enterprise Architecture artefacts and framework documents (see finding 2) are meeting OBS 17 and ensure full compliance by undertaking the reviews in line with planned dates in the tracker, and request that remedial actions are complete by CGI as required.</p> <p>The process should be formalised to ensure the Architectural artefacts required by OBS 17 are in place and available to Digital services.</p> <p>Consideration should also be given to how failure to complete remedial actions will be escalated to ensure compliance. This escalation process should be documented and agreed.</p>	<p>Enterprise Architecture baseline plan will be an agenda item on all EA Boards going forward. The EA plan includes formal checkpoints, facilitating review and progress reporting.</p> <p>Escalation process will be formalised and approved through the EA Board as part of the OLA revision previously agreed.</p>	<p>Deborah Smart, Executive Director of Corporate Services, CEC</p> <p>Mark Bulmer, Vice President Consulting Services, CGI</p>	<p>Nicola Harvey, Service Director, Customer and Digital Services</p> <p>Heather Robb, Chief Digital Officer, Digital Services</p> <p>Mike Bell, Technical Architect, Digital Services</p> <p>Alison Roarty, Commercial Lead, Digital Services</p> <p>Iain Allan, Enterprise Architect, CGI</p>	31/01/2024

# Appendix 1 – Control Assessment and Assurance Definitions

Control Assessment Rating		Control Design Adequacy	Control Operation Effectiveness
Well managed		Well-structured design efficiently achieves fit-for purpose control objectives	Controls consistently applied and operating at optimum level of effectiveness.
Generally Satisfactory		Sound design achieves control objectives	Controls consistently applied
Some Improvement Opportunity		Design is generally sound, with some opportunity to introduce control improvements	Conformance generally sound, with some opportunity to enhance level of conformance
Major Improvement Opportunity		Design is not optimum and may put control objectives at risk	Non-conformance may put control objectives at risk
Control Not Tested	N/A	Not applicable for control design assessments	Control not tested, either due to ineffective design or due to design only audit

## Overall Assurance Ratings

<b>Substantial Assurance</b>	A sound system of governance, risk management and control exists, with internal controls operating effectively and being consistently applied to support the achievement of objectives in the area audited.
<b>Reasonable Assurance</b>	There is a generally sound system of governance, risk management and control in place. Some issues, non-compliance or scope for improvement were identified which may put at risk the achievement of objectives in the area audited.
<b>Limited Assurance</b>	Significant gaps, weaknesses or non-compliance were identified. Improvement is required to the system of governance, risk management and control to effectively manage risks to the achievement of objectives in the area audited.
<b>No Assurance</b>	Immediate action is required to address fundamental gaps, weaknesses or non-compliance identified. The system of governance, risk management and control is inadequate to effectively manage risks to the achievement of objectives in the area audited.

## Finding Priority Ratings

<b>Advisory</b>	A finding that does not have a risk impact but has been raised to highlight areas of inefficiencies or good practice.
<b>Low Priority</b>	An issue that results in a small impact to the achievement of objectives in the area audited.
<b>Medium Priority</b>	An issue that results in a moderate impact to the achievement of objectives in the area audited.
<b>High Priority</b>	An issue that results in a severe impact to the achievement of objectives in the area audited.
<b>Critical Priority</b>	An issue that results in a critical impact to the achievement of objectives in the area audited. The issue needs to be resolved as a matter of urgency.